PCT/JP2004/008682

日本国特許庁
JAPAN PATENT OFFICE

24. 6. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　７月２５日

出願番号
Application Number: 特願２００３－２７９６３７

[ST. 10/C]: [ＪＰ２００３－２７９６３７]

出願人
Applicant(s): 沖電気工業株式会社

２００４年　８月　６日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０７００１３

【書類名】　特許願
【整理番号】　SA003816
【あて先】　特許庁長官殿
【国際特許分類】　G06K　9/36
【発明者】
　【住所又は居所】　東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内
　【氏名】　井戸田　誠一
【特許出願人】
　【識別番号】　000000295
　【氏名又は名称】　沖電気工業株式会社
【代理人】
　【識別番号】　100082050
　【弁理士】
　【氏名又は名称】　佐藤　幸男
【手数料の表示】
　【予納台帳番号】　058104
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9100477

【書類名】特許請求の範囲
【請求項１】
認証対象の身体上の特徴を用いて生体認証し、当該生体認証の結果が肯定的であるときに、その後、当該肯定的な生体認証の結果を前提とした簡易かつ迅速な認証を行える認証媒体を発行する過程と、
前記認証媒体を用いて認証対象を認証し、当該認証媒体による認証の結果に応じて機器の使用を許可する過程とから成ることを特徴とする生体認証併用複合認証方法。
【請求項２】
前記認証媒体は、認証対象である機器使用者の所有物であることを特徴とする請求項１記載の生体認証併用複合認証方法。
【請求項３】
前記認証媒体は、パスワードであることを特徴とする請求項１記載の生体認証併用複合認証方法。
【請求項４】
前記認証媒体である所有物を回収する過程を伴うことを特徴とする請求項２記載の生体認証併用複合認証方法。
【請求項５】
認証対象の身体上の特徴を用いて生体認証する生体認証部と、当該生体認証の結果が肯定的であるときに、認証媒体を発行する媒体発行部とから成る第１の認証装置と、
前記認証媒体を用いて認証対象を認証する媒体認証部と、当該認証媒体による認証の結果に応じて機器の使用を許可する機器制御部から成る第２の認証装置を備えたことを特徴とする生体認証併用複合認証システム。
【請求項６】
前記認証媒体は、認証対象である機器使用者の所有物であることを特徴とする請求項５記載の生体認証併用複合認証システム。
【請求項７】
前記認証媒体は、パスワードであることを特徴とする請求項５記載の生体認証併用複合認証システム。
【請求項８】
前記認証媒体である所有物を回収する回収部を備えたことを特徴とする請求項６記載の生体認証併用複合認証システム。
【請求項９】
前記第１の認証装置は機器使用者の所有物にその後の認証に必要なすべてのデータを書き込み、
前記第２の認証装置は前記所有物から取得したデータのみをもとに単独で機器使用を許可するか否かを判定し得ることを特徴とする請求項６記載の生体認証併用複合認証システム。
【請求項１０】
前記認証媒体である所有物を回収する過程において生体認証を伴うことを特徴とする請求項４記載の生体認証併用複合認証方法。
【請求項１１】
前記認証媒体である所有物を回収する回収部を備えた認識装置内に、当該所有物の回収時に生体認証する生体認証部を備えたことを特徴とする請求項８記載の生体認証併用複合認証システム。

【書類名】明細書
【発明の名称】生体認証併用複合認証方法及びシステム
【技術分野】
【０００１】
本発明は、ICカードや磁気カード等の所有物による個人認証やパスワードによる認証と、バイオメトリクス認証を複合した認証方法及びシステムに関するものである。
【背景技術】
【０００２】
個人認証の方式として従来以下のものがある。
(1)　１つは、所有物による個人認証方式である。これは、ICカードや磁気カードを個人が所有し、そのカードにあらかじめ個人のIDや情報を格納しておくことにより個人認証する方式である。
(2)　もう１つは、バイオメトリクスを利用した個人認証方式である。これは、指紋や虹彩等の個人の身体的特徴を用いる認証方式である。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
図２３において、上述の各認証方式の特徴を比較して示す。図示のように「所有物による個人認証」と「バイオメトリクス個人認証」とは対称的な特徴を示す。
すなわち、「所有物による個人認証」は低費用で認識でき、認証時間が高速であるメリットがある。その反面、悪用される危険性があるとともに、所有物を携帯していないときは認証できないなどのデメリットを有している。
【０００４】
一方、「バイオメトリクス認証」は悪用される危険性が低く、個人の身体特徴のため確実に認証可能であるメリットをもつ。その反面、認証装置が高価となり、認証時間に比較的長時間を要するデメリットを有する。
【課題を解決するための手段】
【０００５】
そこで、本発明は以上の点を解決するため、「所有物による個人認証」と「バイオメトリクス個人認証」を複合することでそれぞれのメリット、デメリットを補うシステムを構成する。
すなわち、次の構成を採用する。
【０００６】
〈構成１〉
１つは、生体認証併用複合認証方法であり、認証対象の身体上の特徴を用いて生体認証し、当該生体認証の結果が肯定的であるときに、その後、当該肯定的な生体認証の結果を前提とした簡易かつ迅速な認証を行える認証媒体を発行する過程と、前記認証媒体を用いて認証対象を認証し、当該認証媒体による認証の結果に応じて機器の使用を許可する過程とから成ることを特徴とする。
これは、１度、安全確実な生体認証を行った後は、簡易かつ迅速な認証を行うようにしたものである。
【０００７】
この方法は、例えば、認証対象の身体上の特徴を用いて生体認証する生体認証部と、当該生体認証の結果が肯定的であるときに、認証媒体を発行する媒体発行部とから成る第１の認証装置と、前記認証媒体を用いて認証対象を認証する媒体認証部と、当該認証媒体による認証の結果に応じて機器の使用を許可する機器制御部から成る第２の認証装置を備えた生体認証併用複合認証システムにおいて使用される。
【０００８】
〈構成２〉
もう１つは、構成１のシステムにおいて、第１の認証装置は機器使用者の所有物にその

後の認証に必要なすべてのデータを書き込み、第２の認証装置は前記所有物から取得したデータのみをもとに単独で機器使用を許可するか否かを判定し得ることを特徴とする。

これは、第１の認証装置と、第２の認証装置とを通信回線で接続できない状況でも、構成１の方法を使用できるシステムである。

【０００９】

〈構成３〉

さらにもう１つは、構成１の方法において、認証媒体である所有物を回収する過程で生体認証を伴うことを特徴とする。

あるいは、構成１または構成２のシステムにおいて、認証媒体である所有物を回収する回収部を備えた認識装置内に、当該所有物の回収時に生体認証する生体認証部を備えたことを特徴とする。

これらは、生体認証を活用して、所有物が機器使用者にとって不要となった後に、その所有物を他の者に利用させることができないような保証を作ろうとするものである。

【発明を実施するための最良の形態】

【００１０】

以下、本発明の最良の実施の形態を実施例を用いて説明する。

【実施例１】

【００１１】

図１は、本発明の実施例１のシステム構成図である。図１において、管理装置11は本システム全体を管理し、所有物あるいはパスワードによる認証と、バイオメトリクス認証を複合した認証を行う。この管理装置11は、認証装置Ａ12、認証装置Ｂ13、認証装置Ｃ14とネットワークで接続されている。

認証装置Ａ12は、バイオメトリクス認証装置12-1と、カード発行装置12-2と、制御機器12-3と、結果表示装置12-4を備えている。

【００１２】

制御機器12-3の例として、電気錠や課金装置があげられる。なお、図示の例では、カード発行装置12-2とともに、制御機器12-3を備えるようにしたが、制御機器を備えない構成でもよい。

結果表示装置12-4は、LEDやLCDを使い使用者に結果を通知する装置である。

使用者は認証装置Ａ12を使い、バイオメトリクス認証を行う。そして、カードを受け取る。この際、図示のような構成のものでは、同時に、ドアの開錠や金銭の支払いをすることができる。

【００１３】

認証装置Ｂ13は、カードリーダ13-1と、制御機器13-2と、結果表示装置13-3を備えている。

制御機器13-2の例として、電気錠や課金装置があげられる。

使用者は認証装置Ｂ13においてカードを使いドアの開錠や支払いをすることができる。

【００１４】

認証装置Ｃ14は、カード回収装置14-1と、制御機器14-2と、結果表示装置14-3を備えている。

カード回収装置14-1は、カードリーダの機能を備えてもよい。

【００１５】

制御機器14-2の例として、電気錠や課金装置があげられる。なお、図示の例では、制御機器14-2を備えたが、制御機器は備えない構成でもよい。

使用者はカード回収装置14-1にてカードを返却する。この際、図示の構成のものでは、同時に、ドアの開錠や金銭の支払いをすることができる。

【００１６】

図２から図５までは、図１の各機器の機能ブロック図である。

図２は、管理装置11の機能ブロック図である。図２において、認証データ受信部101は、認証装置Ａ12からの認証データを受信する。

【００１７】
図６に認証データの一例を示す。認証データは登録者ＤＢ109のＩＤとリンクしているユニークな番号である「ＩＤ」、認証装置Ａ12を識別するための「装置ＩＤ」等の情報から構成される。
図２に戻り、登録者ＤＢ検索部102は、ＩＤをキーにして登録者ＤＢ109からデータを検索する。
【００１８】
図７に登録者ＤＢ109の例を示す。登録者ＤＢ109はユニークな番号である「ＩＤ」、「名前」、カードを発行済みか否かを判定する「カード発行状態」、カードを使用可能な有効期限を示す「カード有効期限」、使用権限のある装置を示す「使用権限」等の情報により構成される。
【００１９】
図２に戻り、カード発行判定部103は、認証データのＩＤで検索された登録者ＤＢ109の「カード発行状態」、「使用権限」等からカード発行するか否かを判定する。カード発行判定の一例としては「カード発行状態」が未発行であり、認証装置Ａ12の使用権限が「使用可」である場合カードを発行可と判定する手法があげられる。
【００２０】
カード発行判定結果送信部104は、カード発行判定の結果およびカード入力データを認証装置Ａ12に送信する。
図８にカード入力データの一例を示す。カード入力データは登録者ＤＢ109のＩＤとリンクしているユニークな番号である「ＩＤ」等の情報により構成される。
【００２１】
図２に戻り、登録者ＤＢ更新部105は、登録者ＤＢ109の「カードの発行状況」と「カード有効期限」等を更新する。
装置データ受信部106は、認証装置Ｂ13または認証装置Ｃ14から装置データを受信する。
【００２２】
図９に装置データを示す。装置データは登録者ＤＢ109のＩＤとリンクしているユニークな番号である「ＩＤ」、装置を識別するために装置毎に固有に与えられた「装置ＩＤ」等の情報により構成される。
【００２３】
図２に戻り、装置使用判定部107は、装置データのＩＤから検索された登録者ＤＢ109の「カード有効期限」および「使用権限」等より、装置の使用を許可するか否かを判定する。装置使用判定の一例としてはカードの有効期限内であり、使用権限が使用可になっている場合があげられる。
【００２４】
装置使用判定結果送信部108は、装置使用判定部107での判定結果を認証装置Ｂ13または認証装置Ｃ14に送信する。
【００２５】
図３は、認証装置Ａ12の機能ブロック図である。図３において、バイオメトリクス認証部121は、図１のバイオメトリクス認証装置12-1を用いて使用者のバイオメトリクスデータを取得する。そして、これを、あらかじめバイオメトリクスＤＢ128に登録されているバイオメトリクスデータとマッチングすることにより使用者を認証する。
【００２６】
図7にバイオメトリクスＤＢ128の一例を示す。バイオメトリクスＤＢは登録者ＤＢ109のＩＤとリンクしているユニークな番号の「ＩＤ」と個人を認証するためのデータである「バイオメトリクスデータ」等の情報から構成されている。図３に示す例では、バイオメトリクスＤＢを認証装置Ａ12に設けたが、管理装置11に設けてネットワークを介して管理装置11においてバイオメトリクス認証を実施してもよい。
【００２７】

結果表示部122は、バイオメトリクス認証の結果やカード発行判定結果等を結果表示装置12-4により使用者に通知する。

【００２８】

認証データ送信部123は、認証データを管理装置11へ送信する。認証データはバイオメトリクスＤＢ128から取得した「ＩＤ」と認証装置Ａ12の装置ＩＤ等からなる（図６参照）。

カード発行判定結果受信部124は、管理装置11から送信されたカード発行判定結果を受信する。

【００２９】

カード発行部125は、カード入力データを書込み、カードをカード発行装置12-2から発行する。

制御部126は、制御機器12-3を制御する。たとえば制御機器12-3が電子錠の場合は電子錠を開錠する。なお、ここでは制御機器12-3を制御するものとしたが、制御機器12-3が備えられていない構成ではカードの発行を実施後、制御機器の制御はしない。

【００３０】

図４は、認証装置Ｂ13の機能ブロック図である。図４において、カードデータ読取り部131は、図１のカードリーダ13-1を用いてカード入力データを読込む。

装置データ送信部132は、装置データを管理装置11へ送信する。装置データはカード入力データおよび装置ＩＤからなる（図９）。

【００３１】

装置使用判定結果受信部133は、図１の管理装置11から装置使用判定結果を受信する。

結果表示部134は、装置使用判定を図１の結果表示装置13-3に表示する。

【００３２】

制御部135は、装置使用判定がＯＫの場合、図１の制御機器13-2を制御する。たとえば、制御機器13-2が電子錠の場合は電子錠を開錠する。

【００３３】

図５は、認証装置Ｃ14の機能ブロック図である。図５において、カードデータ読取り部141は、カード機能を持ったカード回収装置14-1を用いてカード入力データを読込む。

装置データ送信部142は、装置データを管理装置11へ送信する。

【００３４】

装置使用判定結果受信部143は、管理装置11から装置使用判定結果を受信する。

結果表示部144は、装置使用判定を結果表示装置14-4に表示する。

カード回収部145は、カード回収装置14-1を用いてカードを回収する。

【００３５】

制御部146は、装置使用判定がＯＫの場合、制御機器14-2を制御する。たとえば、制御機器14-2が電子錠の場合は電子錠を開錠する。なお、ここではカードのデータにより制御機器を制御しているが、カード回収のみを実施し制御機器の制御は実施しない形態でもよい。また、制御機器を制御するに際しては、カードのデータにより制御機器を制御せずに、カード回収をトリガにして制御機器を制御する手法もある。

【００３６】

〈実施例１の動作〉

図１１、１２、１３における実施例１の動作のフローチャートに沿って、本実施例の動作を説明する。

図１１は、認証装置Ａ12での認証動作を示す。

まず、Ｓ101で、バイオメトリクス認証部121はバイオメトリクス認証を実施する。そして、認証ができた場合はＳ103の処理へ移る。認証ができない場合はＳ102の処理へ移る。

【００３７】

Ｓ102で、結果表示部122は使用者に認証ができなかったことを通知する。

Ｓ103で、認証データ送信部123は認証データを管理装置11に送信する。

【００３８】

ここで、管理装置の動作が始まる。
まず、Ｓ104で、認証データ受信部101は認証データを受信する。
そして、Ｓ105で、登録者ＤＢ検索部102は受信した認証データのＩＤをもとに登録者ＤＢ109上のデータを検索する。
【００３９】
Ｓ106で、カード発行判定部103は検索したデータよりカード発行するか否かを判定する。
また、Ｓ107で、登録者ＤＢ更新部105は登録者ＤＢ109のデータを更新する。
【００４０】
Ｓ108で、カード発行判定結果送信部104は認証装置Ａ12へ結果を送信する。カード発行可の場合はカード発行可の結果とカード入力データを送信する。また、カード発行不可の場合はカード発行不可の結果を送信する。
【００４１】
ここで、認識装置Ａの動作が再開される。
Ｓ109で、カード発行判定結果受信部124はカード発行判定結果を受信する。
Ｓ110で、結果表示部122はカード発行判定結果を使用者に通知する。
Ｓ111で、カード発行部125はカード発行可の場合、Ｓ112の処理へ移る。カード発行不可の場合は終了する。
【００４２】
Ｓ112で、カード発行部125はカード入力データを書込んだカードを発行する。
Ｓ113で、制御部126は所定の動作を実施する。たとえば認証装置Ａに電気錠が設けられているならば電気錠の開錠を実施する。
【００４３】
図１２は、認証装置Ｂ13での認証動作を示す。
まず、Ｓ121で、カードデータ読取り部131は認証装置Ａ12で発行されたカードのカード入力データを読取る。
Ｓ122で、装置データ送信部132は装置データを管理装置11へ送信する。
【００４４】
ここで、管理装置の動作が始まる。
Ｓ123で、装置データ受信部106は装置データを受信する。
Ｓ124で、登録者ＤＢ検索部102は受信した認証データのＩＤをもとに登録者ＤＢ109上のデータを検索する。
Ｓ125で、装置使用判定部107は検索したデータから認証装置Ｂ13の使用許可するか否かを判定する。
Ｓ126で、装置使用判定結果送信部108は認証装置Ｂ13へ結果を送信する。
【００４５】
ここで、認証装置Ｂの動作が再開される。
Ｓ127で、装置使用判定結果受信部133は結果を受信する。
Ｓ128で、結果表示部134は装置使用判定結果を使用者に通知する。
Ｓ129で、制御部135は装置使用可の場合は処理をＳ130へ移す。使用不可の場合は処理を終了する。
Ｓ130で、制御部135は所定の動作を実施する。たとえば、認証装置Ｂ13に電気錠が設けられているならば電気錠の開錠を実施する。
【００４６】
図１３は、認証装置Ｃ14での認証動作を示す。
まず、Ｓ141で、カードデータ読取り部141は認証装置Ａ12で発行されたカードのカード入力データを読取る。
Ｓ142で、装置データ送信部142は装置データを管理装置11へ送信する。
【００４７】
ここで、管理装置の動作が始まる。

Ｓ143で、装置データ受信部106は装置データを受信する。
Ｓ144で、登録者ＤＢ検索部102は受信した認証データのＩＤをもとに登録者ＤＢ109上のデータを検索する。
Ｓ145で、装置使用判定部107は検索したデータから認証装置Ｃ14の使用許可するか否かを判定する。
Ｓ146で、装置使用判定結果送信部108は認証装置Ｃ14へ結果を送信する。
【００４８】
ここで、認証装置Ｃの動作が再開される。
Ｓ147で、装置使用判定結果受信部143は結果を受信する。
Ｓ148で、結果表示部144は装置使用判定結果を使用者に通知する。
Ｓ149で、カード回収部145は装置使用可の場合は処理をＳ151へ移す。使用不可の場合はＳ150へ処理を移す。
【００４９】
Ｓ150で、カード回収部145はカードを使用者に返却する。これにより、処理終了する。
Ｓ151で、カード回収部145はカードを回収する。
Ｓ152で、制御部135は所定の動作を実施する。たとえば、認証装置Ｃ14に電気錠が設けられているならば電気錠の開錠を実施する。
【００５０】
なお、上述した実施例においては、カード等の所有物による認証とバイオメトリクス認証を複合させるものについて説明したが、本発明はこれに限らず、暗証すなわちパスワードによる認証とバイオメトリクス認証を複合させたものによっても同様に実現できるものである。この点、後述する実施例についても同様である。
【００５１】
〈実施例１の効果〉
以上詳述したように、実施例１のシステムによりバイオメトリクス認証と所有物による認証の両方の利便性を得ることが可能となる。すなわち、本システムによりバイオメトリクス認証による安全性および随時携帯しなくてよいという利便性を得るとともに、所有物による認証による即座に認証可能であるという利便性を得ることが可能となる。
【００５２】
例えば、会社等の施設での運用を考える。会社の門では認証装置Ａ12でバイオメトリクス認証を実施し、カードを取得する。ここでは、バイオメトリクス認証を実施するため高い安全性を確保できる。この際、カードはこの場で発行されるため、カードを携帯する必要はない。会社内ではこのカードと認証装置Ｂ13を使う。このカードで食堂での支払いや、入退室管理を実施する。バイオメトリクスでは照合に時間がかかるケースがあるため食堂等で混雑する可能性があるが、カードは即座に認証可能なため混雑することはない。このカードは最後会社から退社する際に認証装置Ｃ14で回収する。従って会社の外にカードがもちだされることはないため盗難等の危険性は低い。
【００５３】
また、本システムをマンションの管理システムに応用した場合には、マンションの入口で本システムに登録された住民は認証装置Ａ12によりバイオメトリクス認証を受け、カードあるいはキーを取得する。ここで、バイオメトリクス認証の実施により高度のセキュリティを確保できる。この際、カードやキーはこの場で発行されるため、それらを携帯して外出する必要はない。自宅に入るときはこのカードあるいはキーと認証装置Ｂ13を使う。このカードやキーは外出する際にマンションの出口に設けられた認証装置Ｃ14で回収する。従ってマンションの外にこれらがもちだされることはないため盗難等の危険性は低くなる。
【実施例２】
【００５４】
図１４は、実施例２のシステム構成図である。実施例１と異なる点は管理装置11と認証装置Ａ12はネットワークで接続されているが、認証装置Ｂ13と認証装置Ｃ14は管理装置11

に接続されていない点である。その他の構成は実施例１と同様である。

【００５５】

図１５および１６は、各機器の機能ブロック図である。管理装置と認証装置Ａの機能ブロック図は、実施例１と同様である。図１７は、実施例２でのカード入力データの一例である。カード入力データはユニークな番号である「ＩＤ」、カードを使用可能な有効期限を示す「カード有効期限」、使用権限のある装置を示す「使用権限」等の情報により構成される。

【００５６】

図１５は、認証装置Ｂ13の機能ブロック図である。図１５において、カードデータ読取り部231は、カードリーダ13-1を用いてカード入力データを読込む。装置使用判定部232は、「カード有効期限」、「使用権限」等より装置の使用を許可するか否かを判定する。装置使用判定の一例としてはカード有効期限内であり、装置毎に割り当てられている「装置ＩＤ」の使用権限が使用可の場合、使用を許可する手法があげられる。

【００５７】

結果表示部233は、装置使用判定部232における結果を結果表示装置13-3に表示する。制御部234は、装置使用判定がＯＫの場合、制御機器13-2を制御する。たとえば、制御機器13-3が電子錠の場合は電子錠を開錠する。

【００５８】

図１６は、認証装置Ｃ14の機能ブロック図である。図１６において、カードデータ読取り部241は、カード機能を持ったカード回収装置14-3を用いてカード入力データを読込む。装置使用判定部242は、「カード有効期限」、「使用権限」等より装置の使用を許可するか否かを判定する。

【００５９】

結果表示部243は、装置使用判定を結果表示装置14-4に表示する。カード回収部244は、カード回収装置14-1を用いてカードを回収する。制御部245は、装置使用判定がＯＫの場合、制御機器14-3を制御する。たとえば、制御機器14-3が電子錠の場合は電子錠を開錠する。

【００６０】

〈実施例２の動作〉

図１８および１９の実施例２の動作のフローチャートに沿って、本実施例の動作を説明する。

実施例１における図１１のＳ101～Ｓ113までの動作は実施例２も同じように行われるものである。ただし、カード入力データが図１７の内容になる。

【００６１】

図１８は、認証装置Ｂ13での認証動作である。

まず、Ｓ221で、カードデータ読取り部231は認証装置Ａ12で発行されたカードのカード入力データを読取る。

Ｓ222で、装置使用判定部232はカード入力データから認証装置Ｂ13の使用許可するか否かを判定する。

そして、Ｓ223で、結果表示部233は装置使用判定結果を使用者に通知する。

【００６２】

Ｓ224で、制御部234は装置使用可の場合は処理をＳ225へ移す。使用不可の場合は処理を終了する。

Ｓ225で、制御部234は所定の動作を実施する。たとえば、認証装置Ｂ13に電気錠が設けられているならば電気錠の開錠を実施する。

【００６３】

図１９は、認証装置Ｃ14での認証動作を示す。

まず、Ｓ241で、カードデータ読取り部241は認証装置Ａ12で発行されたカードのカード入力データを読取る。

Ｓ242で、装置使用判定部242はカード入力データから認証装置Ｃ14を使用許可するか否

かを判定する。
そして、Ｓ243で、結果表示部243は装置使用判定結果を使用者に通知する。
【００６４】
Ｓ244で、カード回収部244は装置使用可の場合は処理をＳ246へ移す。使用不可の場合はＳ245へ処理を移す。
Ｓ245で、カード回収部244はカードを使用者に返却する。これで、処理を終了する。
Ｓ246で、カード回収部244はカードを回収する。
【００６５】
Ｓ247で、制御部245は所定の動作を実施する。たとえば、認証装置Ｃ14に電気錠が設けられているならば電気錠の開錠を実施する。
【００６６】
〈実施例２の効果〉
以上詳述したように、実施例２によれば、実施例１と異なり、以下の効果がある。すなわち、実施例１では認証装置Ｂ13と認証装置Ｃ14がネットワークに接続されている必要があったが、実施例２では、これらの装置はネットワークとは接続されていない。このため、これらの装置をネットワークにつなげることができないような環境でも、実施例１と同様の効果を得られる。
【００６７】
例えばコンドミニアムの運用を考える。コンドミニアムがある場所はネットワーク環境が整備されていないような場所とする。使用者は認証装置Ａ11を使いカードを取得する。認証装置Ａ11はネットワーク接続可能な場所に設置されている。このカードを認証装置Ｂ13が設置されているコンドミニアムで使用することでコンドミニアムの錠を開錠でき、設備の使用が可能となる。
【実施例３】
【００６８】
図２０は実施例３のシステム構成図である。実施例１と異なる点は認証装置Ｃ14にバイオメトリクス認証装置が備えられたことである。管理装置11と認証装置Ａ12と認証装置Ｂ13は実施例１と同様である。
【００６９】
認証装置Ｃ34は、バイオメトリクス認証装置34-1と、カード回収装置34-2と、制御機器34-3と、結果表示装置34-4を備えている。ここでは、実施例１の構成に認証装置Ｃ34を備えたが、実施例２の構成に認証装置Ｃ34を備えてもよい。
【００７０】
図２１は各機器の機能ブロック図である。管理装置11と認証装置Ａ12と認証装置Ｂ13は実施例１の機能ブロック図と同様である。
そこで、図２１では認証装置Ｃ34の機能ブロックのみを示す。図２１において、バイオメトリクス認証部341は、バイオメトリクス認証装置34-1を用いて使用者のバイオメトリクスデータを取得し、あらかじめバイオメトリクスＤＢ349に登録されているバイオメトリクスデータとマッチングすることにより使用者を認証する。
【００７１】
カードデータ読取り部342は、カードリーダ機能を持ったカード回収装置34-2を用いてカード入力データを読込む。カード所有者判定部343は、カード内のIDとバイオメトリクス認証で取得できたIDが一致するか否かを判定する。装置データ送信部344は、装置データを管理装置11へ送信する。装置使用判定結果受信部345は、管理装置11から装置使用判定結果を受信する。
【００７２】
結果表示部346は、装置使用判定を結果表示装置34-4に表示する。カード回収部347は、カード回収装置34-2を用いてカードを回収する。制御部348は、装置使用判定がＯＫの場合、制御機器34-3を制御する。たとえば、制御機器34-3が電子錠の場合は電子錠を開錠する。ここではカードのデータにより制御機器を制御しているが、カード回収をトリガにし

て制御機器を制御する手法や、カード回収のみを実施し、制御機器の制御は実施しない形態でもよい。

【００７３】

〈実施例３の動作〉

実施例１における図１１のＳ101～Ｓ113、図１２のＳ121～Ｓ130までの動作は実施例３でも同じである。

【００７４】

図２２は認証装置Ｃ34での認証動作を示す。

まず、Ｓ341で、バイオメトリクス認証部341はバイオメトリクス認証を実施する。認証ができた場合はＳ343の処理へ移る。認証ができない場合はＳ342の処理へ移る。

Ｓ342で、結果表示部346は認証結果ＮＧを使用者に通知する。そして、ここで処理を終了する。

【００７５】

一方、Ｓ343で、結果表示部346は認証結果ＯＫを使用者に通知する。

Ｓ344で、カードデータ読取り部342は認証装置Ａ12で発行されたカードのカード入力データを読取る。

Ｓ345で、カード所有者判定部343はバイオメトリクス認証で得られたIDとカード入力データのIDが一致するか否かを判定する。そして、一致する場合はS347の処理へ移行する。一致しない場合はS346の処理へ移行する。

【００７６】

Ｓ346で、結果表示部346はIDが一致しないことを使用者に通知する。

Ｓ347で、装置データ送信部344は装置データを管理装置11へ送信する。これにより、管理装置での処理が始められる。

【００７７】

Ｓ348で、装置データ受信部106は装置データを受信する。

Ｓ349で、登録者ＤＢ検索部102は受信した認証データのＩＤをもとに登録者ＤＢ109上のデータを検索する。

Ｓ350で、装置使用判定部107は検索したデータから認証装置Ｃ34の使用許可するか否かを判定する。

Ｓ351で、装置使用判定結果送信部108は認証装置Ｃ34へ結果を送信する。これにより、認証装置Ｃの動作が再開される。

【００７８】

Ｓ352で、装置使用判定結果受信部345は結果を受信する。

Ｓ353で、結果表示部346は装置使用判定結果を使用者に通知する。

Ｓ354で、カード回収部347は装置使用可の場合は処理をＳ356へ移す。使用不可の場合はＳ355へ処理を移す。

Ｓ355で、カード回収部347はカードを使用者に返却する。これで処理を終了する。

【００７９】

Ｓ356では、カード回収部347はカードを回収する。

Ｓ357で、制御部348は所定の動作を実施する。たとえば、認証装置Ａに電気錠が設けられているならば電気錠の開錠を実施する。

【００８０】

〈実施例３の効果〉

実施例３によりある人がバイオメトリクス認証を実施して取得したカードを第三者が取得して不正利用することを防止することができる。

【００８１】

例としてスキー場のリフト券を考える。スキー場ではリフト券の転売問題が存在する。ある人が購入したリフト券を第三者に転売することで同じリフト券で２名以上が使用する問題である。認証装置Ｃ34を使用することでそのリフト券が購入者のものか否かを判定できるため転売問題のような不正利用を防止できる。

【００８２】
具体的には、リフト券の購入時に認証装置Ａでその購入者から保証金を預かり、認証装置Ｃでリフト券の返還を条件としてバイオメトリクス認証で確認したその購入者にその保証金を返すようにする。

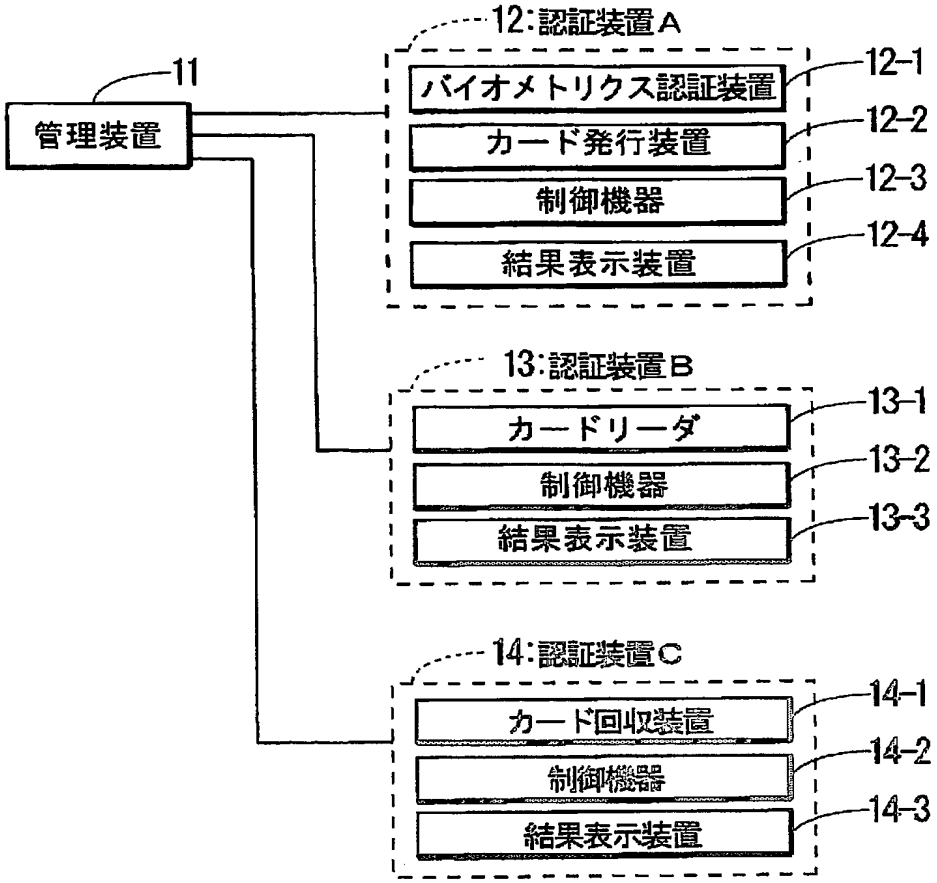
【図面の簡単な説明】

【００８３】
【図１】本発明の実施例１のシステム構成を示すブロック図である。
【図２】図１の管理装置の機能構成を示すブロック図である。
【図３】図１の認証装置Ａの機能構成を示すブロック図である。
【図４】図１の認証装置Ｂの機能構成を示すブロック図である。
【図５】図１の認証装置Ｃの機能構成を示すブロック図である。
【図６】認証データの一例を示す図である。
【図７】登録者ＤＢの一例を示す図である。
【図８】カード入力データの一例を示す図である。
【図９】装置データの一例を示す図である。
【図１０】バイオメトリクスデータの一例を示す図である。
【図１１】認証装置Ａでの認証動作を示すフローチャートである。
【図１２】認証装置Ｂでの認証動作を示すフローチャートである。
【図１３】認証装置Ｃでの認証動作を示すフローチャートである。
【図１４】本発明の実施例２のシステム構成を示すブロック図である。
【図１５】図１４の認証装置Ｂの機能構成を示すブロック図である。
【図１６】図１４の認証装置Ｃの機能構成を示すブロック図である。
【図１７】実施例２でのカード入力データの一例を示す図である。
【図１８】実施例２の認証装置Ｂでの認証動作を示すフローチャートである。
【図１９】実施例２の認証装置Ｃでの認証動作を示すフローチャートである。
【図２０】本発明の実施例３のシステム構成を示すブロック図である。
【図２１】図２０の認証装置Ｃの機能構成を示すブロック図である。
【図２２】実施例３の認証装置Ｃでの認証動作を示すフローチャートである。
【図２３】所有物による認証とバイオメトリクス認証との比較内容の説明図である。

【符号の説明】

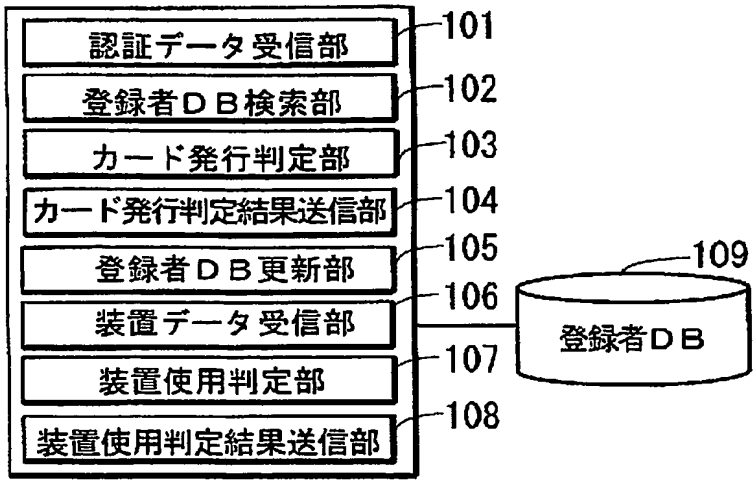
【００８４】
１１　管理装置
１２　認証装置Ａ
１３　認証装置Ｂ
１４　認証装置Ｃ

【書類名】図面
【図１】



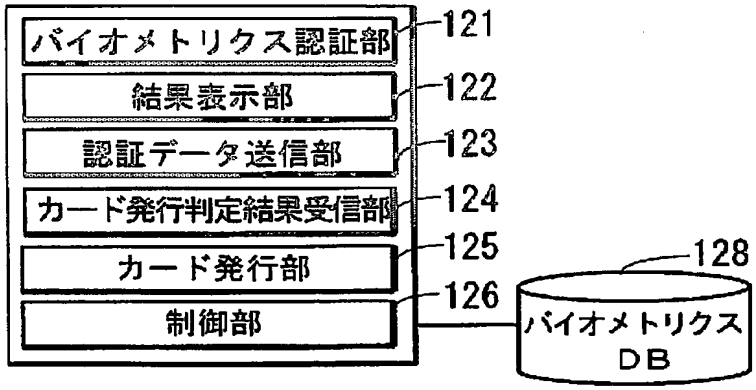
本発明の実施例１のシステム

【図２】



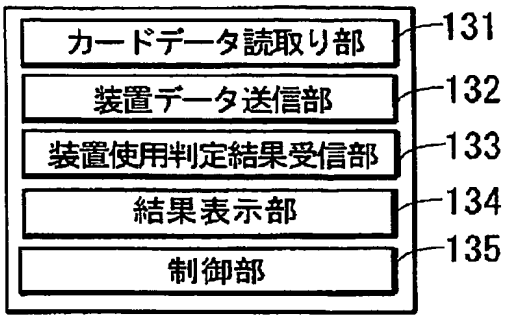
管理装置の機能構成

【図３】



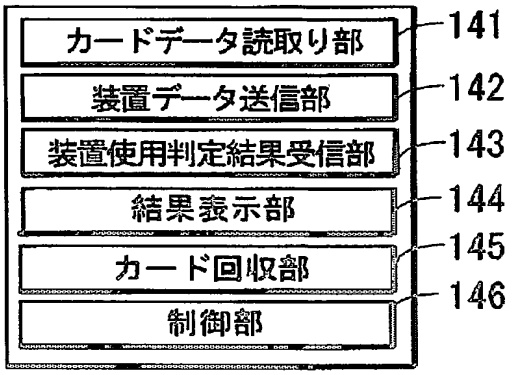
認証装置Ａの機能構成

【図４】



認証装置Ｂの機能構成

【図５】



認証装置Ｃの機能構成

【図６】

ＩＤ	装置ＩＤ
ＸＸＸＸＸＸ	ＡＡＡＡＡＡ
ＸＸＸＸＸＸ	ＡＡＡＡＡＡ
・	

認証データの一例

【図７】

ID	名前	カード発行状態	カード有効期限	使用権限		
				装置ID1	装置ID2	・
XXXXXX	沖　太郎	未発行	――――	使用可	使用可	・
XXXXXX	山田　次郎	発行	hh:mm:ss	使用不可	使用可	・
・	・	・	・	・	・	・

登録者ＤＢの一例

【図８】

ＩＤ
ＸＸＸＸＸＸ
ＸＸＸＸＸＸ
・

カード入力データの一例

【図９】

ＩＤ	装置ＩＤ
ＸＸＸＸＸＸ	ＡＡＡＡＡＡ
ＸＸＸＸＸＸ	ＡＡＡＡＡＡ
・	・

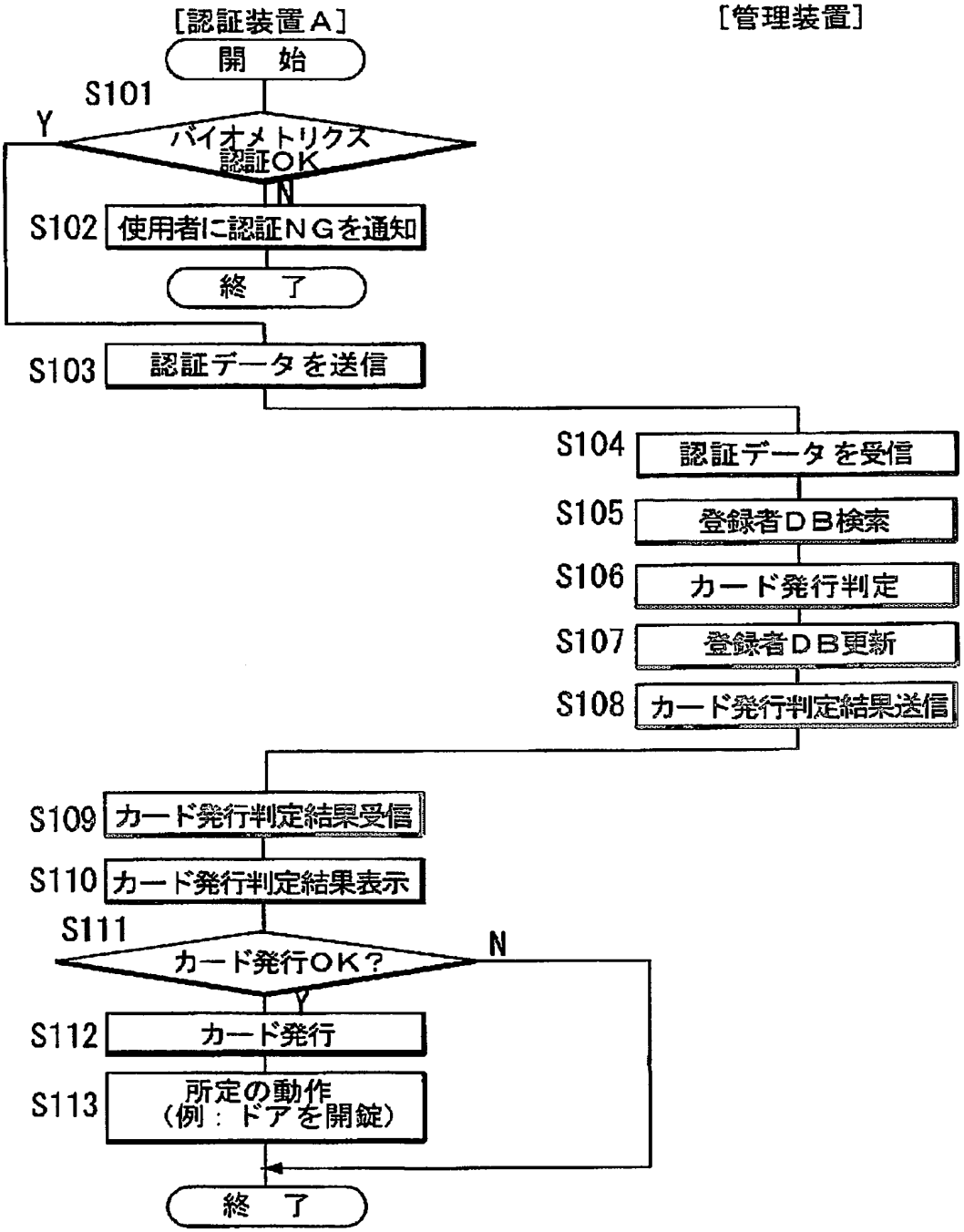
装置データの一例

【図１０】

ＩＤ	バイオメトリクスデータ
ＸＸＸＸＸＸ	＊＊＊＊＊＊＊＊＊＊
ＸＸＸＸＸＸ	＊＊＊＊＊＊＊＊＊＊
・	・

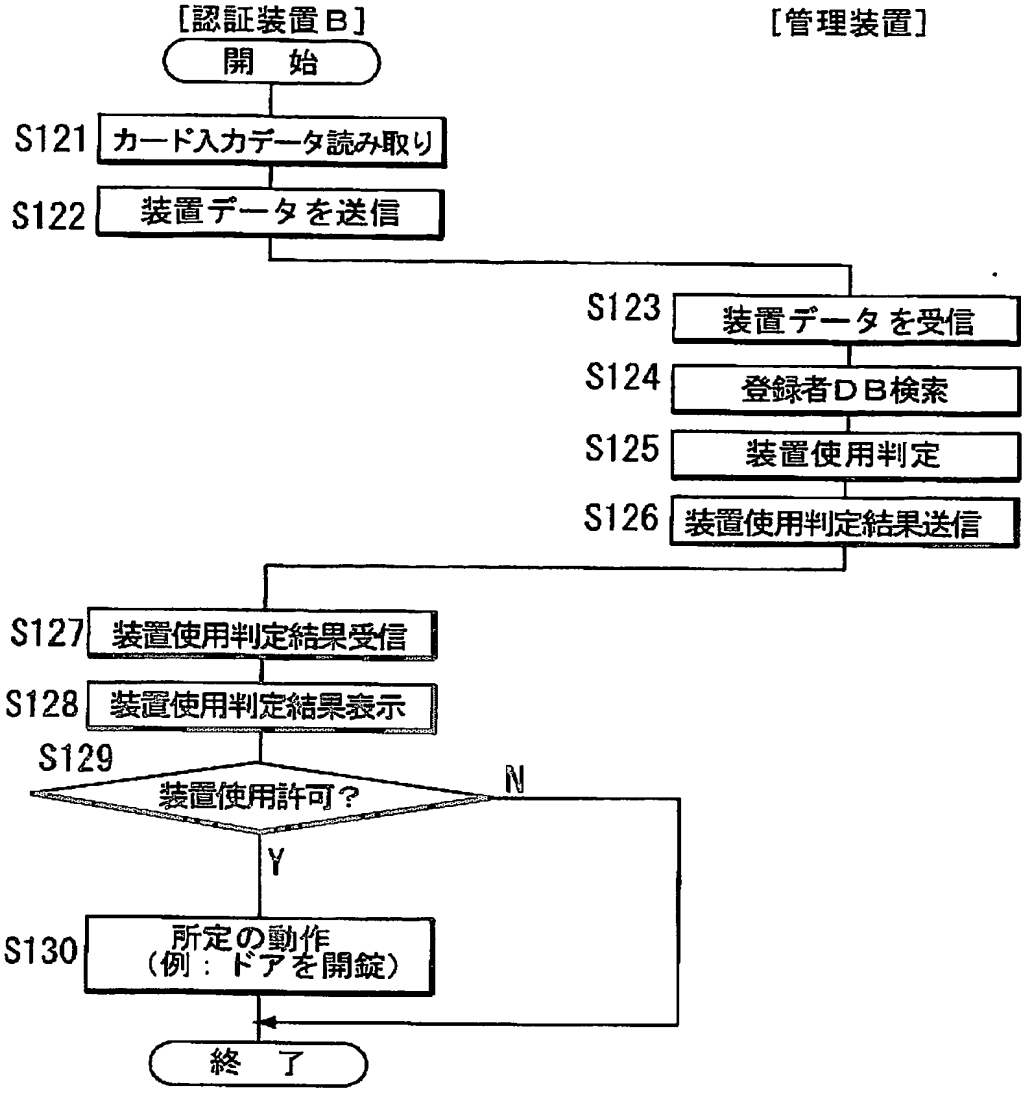
バイオメトリクスデータの一例

【図１１】



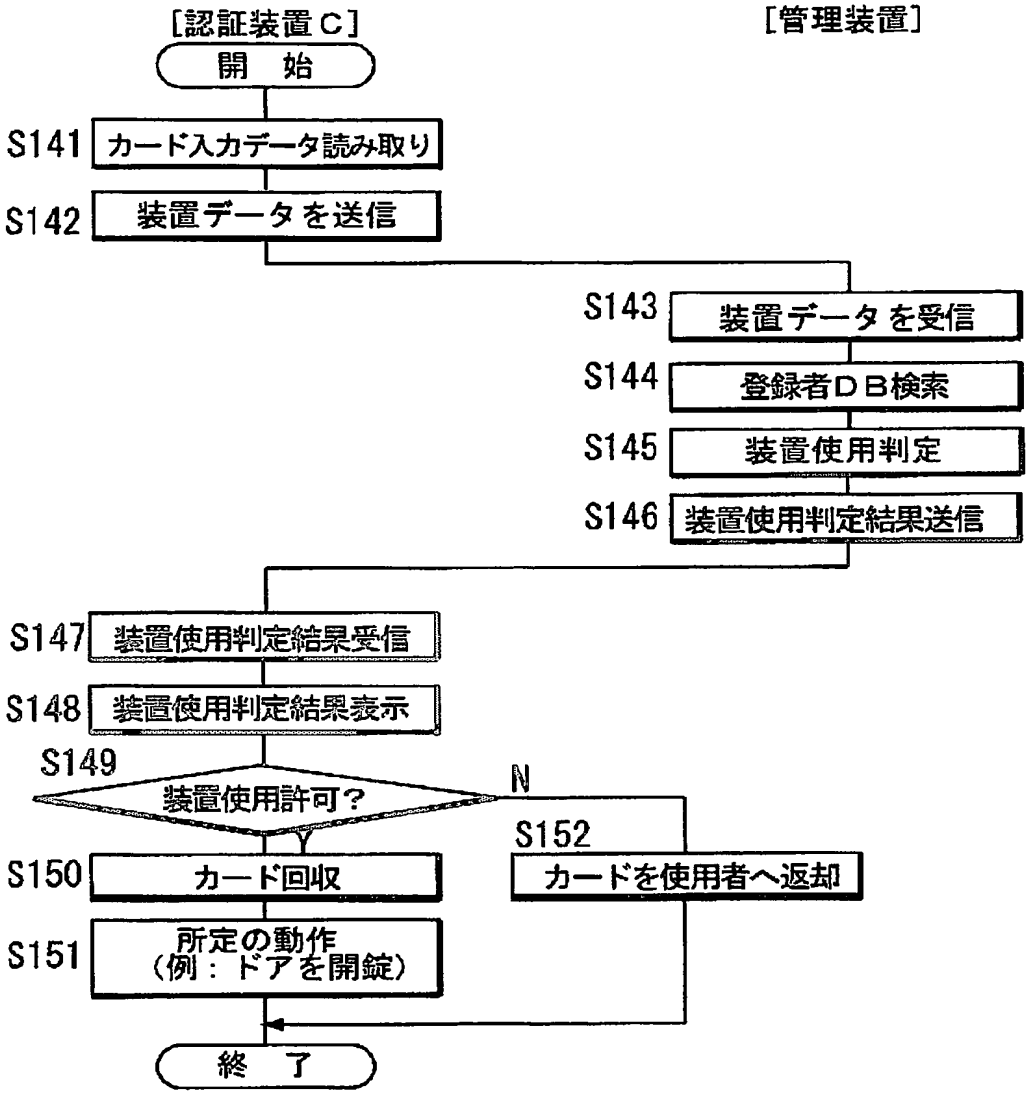
実施例１の認証装置Ａでの認証動作

【図１２】



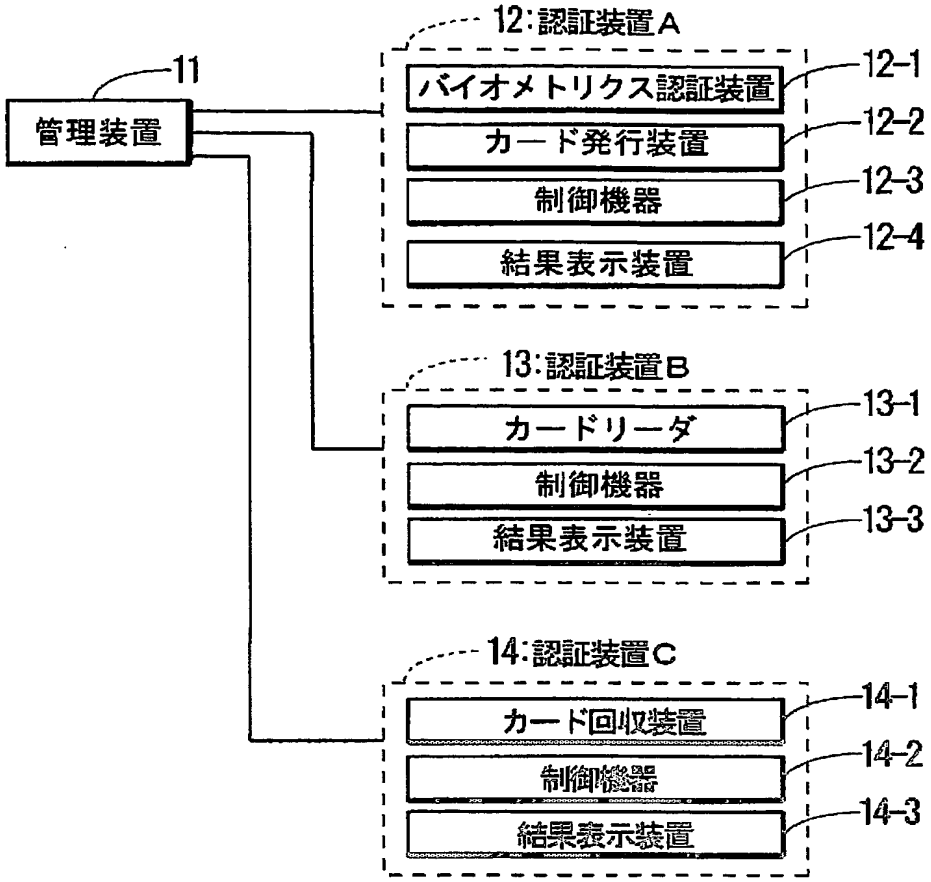
実施例１の認証装置Ｂでの認証動作

【図１３】



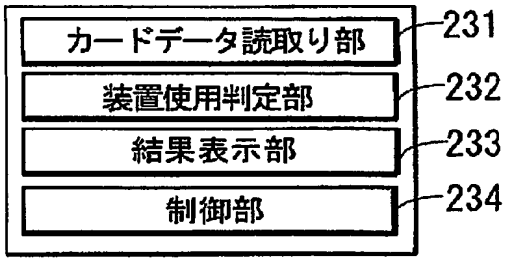
実施例１の認証装置Ｃでの認証動作

【図１４】



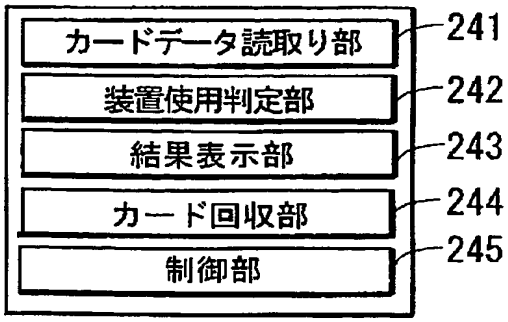
本発明の実施例２のシステム

【図１５】



認証装置Bの機能構成

【図１６】



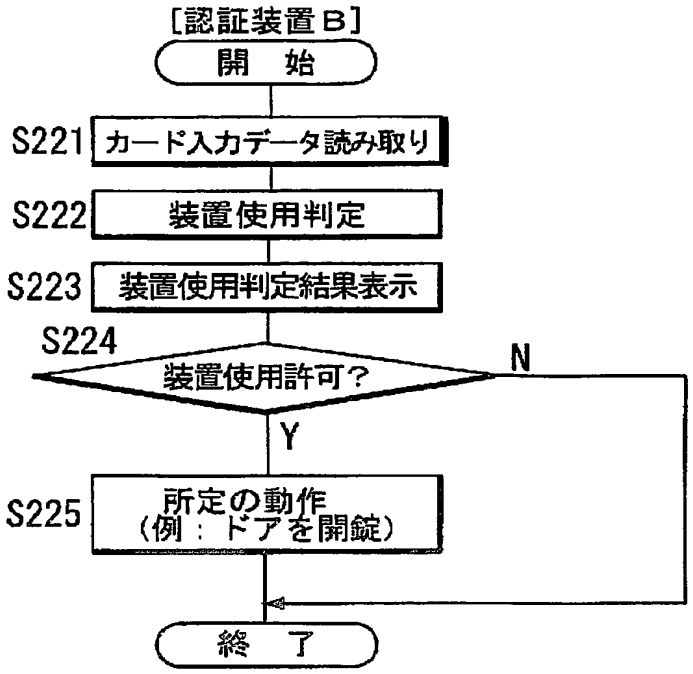
認証装置Ｃの機能構成

【図１７】

ID	カード	使用権限		
	有効期限	装置ID1	装置ID2	・
XXXXXX	―――	使用可	使用可	・
XXXXXX	hh:mm:ss	使用不可	使用可	・
・	・	・	・	・

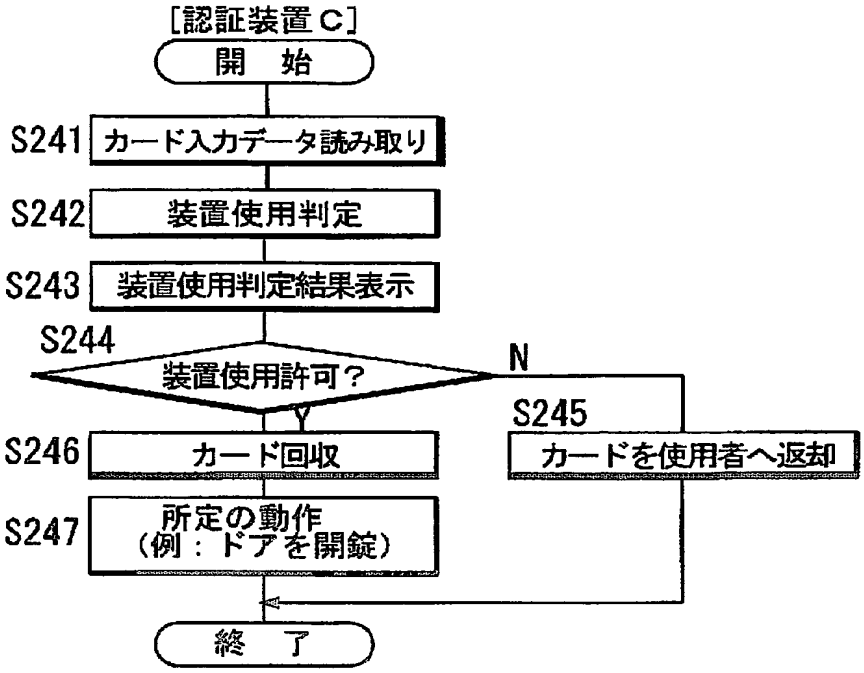
カード入力データの一例

【図１８】



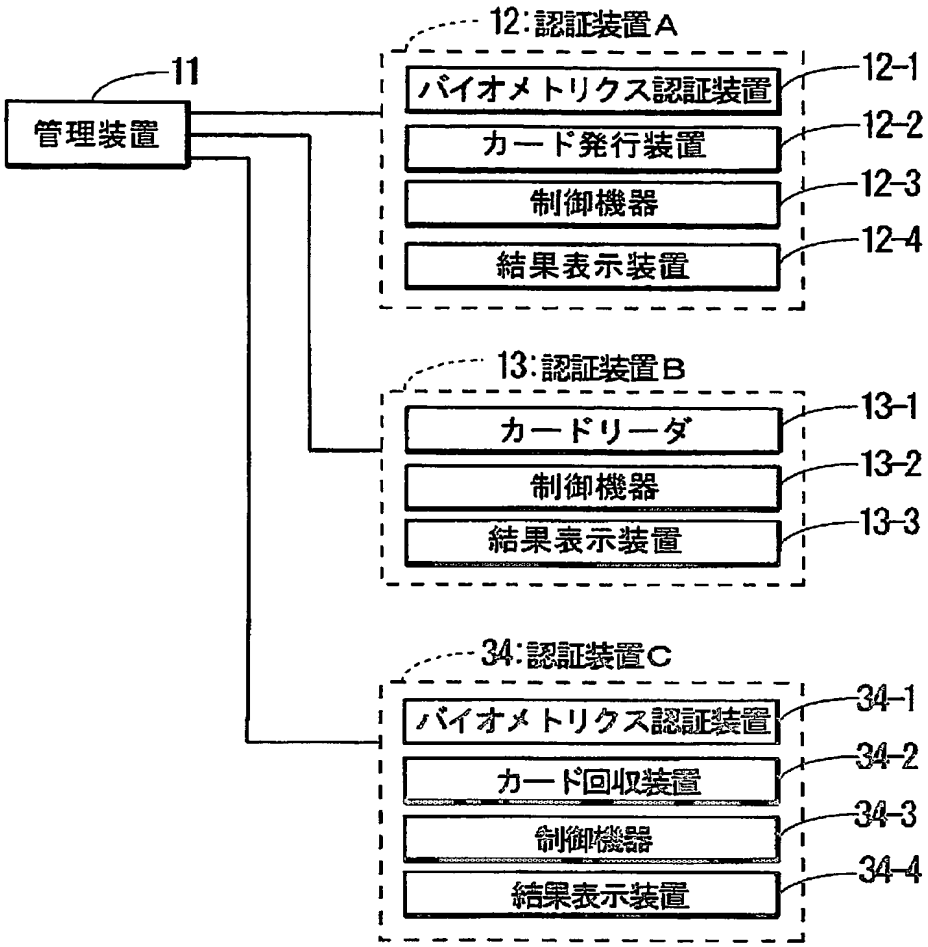
実施例２の認証装置Ｂでの認証動作

【図１９】



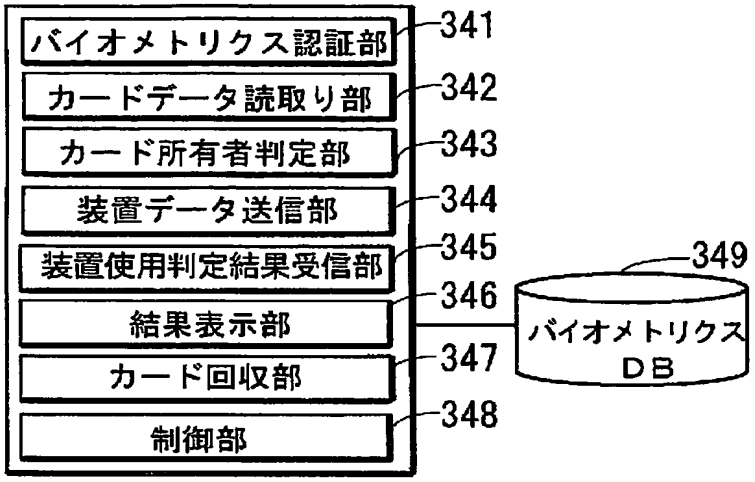
実施例２の認証装置Ｃでの認証動作

【図２０】



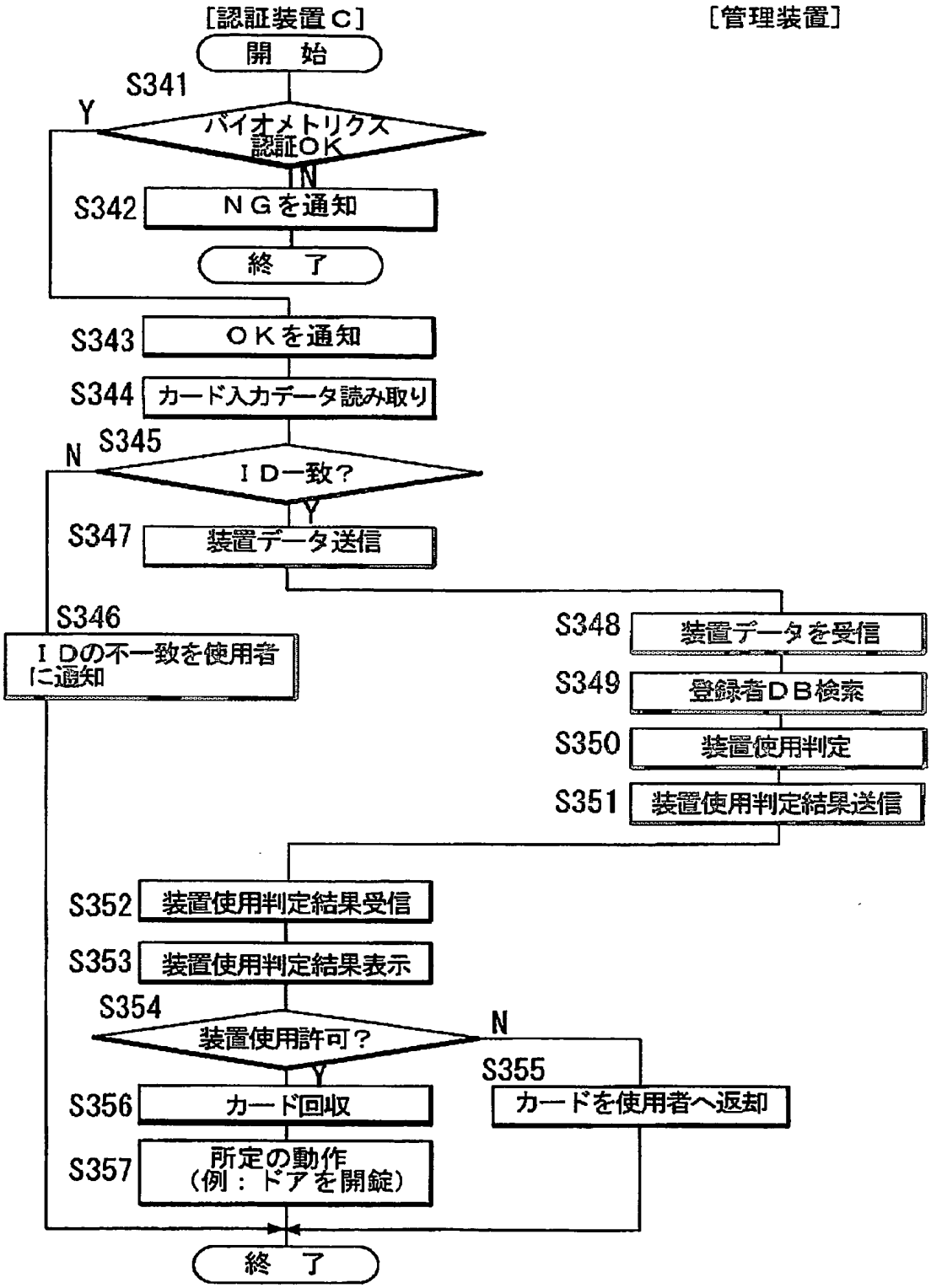
本発明の実施例３のシステム

【図２１】



実施例３の認証装置Ｃの機能構成

【図２２】



実施例３の認証装置Ｃでの認証動作

【図２３】

	所有物	バイオメトリクス
	磁気カード、ＩＣカードなど	指紋、虹彩、顔貌など
費用の安さ	○	× ・所有物による個人認証に比べ高価
悪用の困難さ	× ・紛失盗難の恐れがある	◎ ・偽造は困難
認証時間の速さ	○	△ ・認証に時間を要するケースがある
確実な認証	△ ・所有物の携帯を忘れた場合認証不可	◎ ・身体特徴のため確実に認証可能

所有物による認証とバイオメトリクス認証との比較

【書類名】要約書
【要約】
【課題】生体認証と通常の認証との双方の利点を引き出す。
【解決手段】生体認証併用複合認証システムは、少なくとも、第１の認証装置Ａ１２と、第２の認証装置Ｂ１３とを備え、これらを管理する管理装置１１を備える。第１の認証装置Ａ１２は、認証対象である機器使用者の身体上の特徴を用いて生体認証するバイオメトリクス認証装置12-1と、当該生体認証の結果が肯定的であるときに、認証媒体であるカードを発行するカード発行装置12-2とを含む。第２の認証装置Ｂ１３は、前記カードを用いて使用者を認証するために当該カードを読み取るカードリーダ13-1と、当該カードによる認証の結果に応じて機器の使用を許可する制御機器13-2とを含む。これらの装置を各方式の認証の特性に応じて使い分ける。なお、カードは、認証装置Ｃ１４に設けられたカード回収装置14-1で回収するようにしても良い。
【選択図】図１

認定・付加情報

特許出願の番号	特願２００３－２７９６３７
受付番号	５０３０１２２８９６３
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　７月２８日

＜認定情報・付加情報＞

【提出日】　平成15年 7月25日

特願２００３－２７９６３７

出　願　人　履　歴　情　報

識別番号　［０００００２９５］

１．変更年月日　１９９０年　８月２２日
［変更理由］　新規登録
住　所　東京都港区虎ノ門１丁目７番１２号
氏　名　沖電気工業株式会社